PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY : DoD Instruction 5400.16, DoD Privacy Impact Assessment (PIA) Guidance

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

DISA Service Platform (DSP)

2. DOD COMPONENT NAME:

Defense Information Systems Agency

3. PIA APPROVAL DATE:

10/12/2022

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: Federal contractors, military family members, and foreign nationals are included in general public.)*

- ☐ From members of the general public
- ☐ From Federal employees
- ☒ from both members of the general public and Federal employees
- ☐ Not Collected *(if checked proceed to Section 4)*

b. The PII is in a: *(Check one.)*

- ☒ New DoD Information System
- ☐ New Electronic Collection
- ☐ Existing DoD Information System
- ☐ Existing Electronic Collection
- ☐ Significantly Modified DoD Information System

c. Describe the purpose of this DoD information system or electronic collection and describe the types of personal information about individuals collected in the system.

DISA Service Platform (DSP) is DISA's instantiation of the ServiceNow SaaS cloud offering. Currently, Customer Relationship Management (CRM), Global Service Desk - Information Technology Service Management+ (GSD-ITSM+) and DISA Marketplace (DMP) are fielded on the platform. Account Tracking and Automation Tool (ATAT) is currently under development within a DMP sandbox environment. DSP will be used to manage and track technical issues, service requests and Mission Partner engagement. DSP uses PKI enabled single sign on authentication services for user authentication. The Test and Development environments are hosted by ServiceNow GCC. The user's DoD ID Number (EDPI number), Name, Home/Cellphone, Work Email Address, Official Duty Address, Official Duty Telephone phone, Position/Title, and Rank/Grade is retained within the system for the creation of the accounts and cloud portfolios.

d. Why is the PII collected and/or what is the intended use of the PII? *(e.g., verification, identification, authentication, data matching, mission-related use, administrative use)*

DMP: PII is collected from users during user registration and also when completing / creating an order form, where key service related POCs are identified on the service request. DMP will also leverage the GFUD authentication capabilities currently employed in DSP. DSP has downloaded and stored millions of user records from GFUD or DCMD containing PII contact information, so DMP would leverage that PII data as well. All DSF users have access to PII information, but order data containing PII is restricted to orders submitted by users within their agency. However, all users have access to the DSF Central Address Directory (CAD) where they can look up any registered DSF user regardless of agency. Lastly, POC and location management functions, and via viewing details of a service order.

ATAT: The user's DoD ID Number (EDPI number), Name, Home/Cellphone, Work Email Address, Official Duty Address, Official Duty Telephone phone, Position/Title, and Rank/Grade is retained within the system for the creation of the cloud portfolios.

CRM: PII will be used to facilitate continued conversations between missions partners and the DISA Mission Partner Engagement Office (MPEO).

ITSM+: PII will be used to address tickets and service requests submitted by DoD users via the Global Service Desk.

e. Do individuals have the opportunity to object to the collection of their PII? ☒ Yes ☐ No

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object to the collection of PII.

Individuals can object to the collection of their PII by not completing and submitting the information required.

f. Do individuals have the opportunity to consent to the specific uses of their PII? ☒ Yes ☐ No

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

Individuals can object to the specific uses of their PII by not completing and submitting the information required.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. *(Check as appropriate and provide the actual wording.)*

☐ Privacy Act Statement ☒ Privacy Advisory ☐ Not Applicable

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.
By using this IS (which includes any device attached to this IS), you consent to the following conditions:

The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
At any time, the USG may inspect and seize data stored on this IS.
Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.
Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

h. With whom will the PII be shared through data/system exchange, both within your DoD Component and outside your Component? *(Check all that apply)*

☒	Within the DoD Component	Specify.	DISA
☒	Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	All DoD Agencies
☒	Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	All Federal Agencies
☐	State and Local Agencies	Specify.	

☒ Contractor *(Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)*

Specify.

DISA Market Place (DMP):
- Indrasoft (an ECS owned Company)
- SAIC
- Intellect Solutions
- Norseman Defense Technologies
- Column Highmetric (changed to MajorKey and then bought by New Rocket)
- ONYX

* Contract is being modified to include the mandatory 52.224-1 and 52.224-2 privacy act clauses.

MPEO CRM:
- Norseman Defense Technologies

* Contract is being modified to include the mandatory 52.224-1 and 52.224-2 privacy act clauses.

ITSM+:
Carahsoft
Norseman Defense Technologies
New Rocket

* ITSM+ is under the CRM contract which is being modified to include the mandatory 52.224-1 and 52.224-2 privacy act clauses.

ATAT:
Hunter Strategy

* ATAT falls under the DMP Contract which is being modified to include the mandatory 52.224-1 and 52.224-2 privacy act clauses.

☐ Other *(e.g., commercial providers, colleges).*

Specify.

i. Source of the PII collected is: *(Check all that apply and list all information systems if applicable)*

☒ Individuals
☒ Existing DoD Information Systems
☐ Other Federal Information Systems
☒ Databases
☐ Commercial Systems

Global Federated User Domain (GFUD)

j. How will the information be collected? *(Check all that apply and list all Official Form Numbers if applicable)*

☒ E-mail
☐ In-Person Contact
☐ Fax
☒ Information Sharing - System to System
☒ Other *(If Other, enter the information in the box below)*
☐ Official Form (*Enter Form Number(s) in the box below)*
☐ Paper
☒ Telephone Interview
☒ Website/E-Form

Global Federated User Domain (GFUD)

k. Does this DoD Information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information must be consistent.

☒ Yes ☐ No

If "Yes," enter SORN System Identifier K890.14

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.defense.gov/Privacy/SORNs/

or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority. GRS 5.8 (DAA-GRS-2017-0001- 0001)

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

Temporary. Destroy 1 year after resolved, or when no longer needed for business use, whichever is appropriate.

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statue or Executive Order.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply).

(a) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) If direct or indirect authority does not exist, DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component must be identified.

The following authority allows DISA Service Platform (DSP) to collect the following data: U.S.C. Chapter 8-Defense Agencies and Department of Defense Field Activities; DoD Directive (DoDD) 5105.19, Defense Information Systems Agency (DISA); DoD Directive 1000.25, DoD Personnel Identity Protection (PIP) Program; DoD Global Information Grid 2.0 Concept of Operations (GIG 2.0 CONOPS); DoDI 5200.46-"DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC)" and DoDI 8520.03-Identity Authentication for Information Systems

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (OMB) Control Number?

Contact the Component Information Management Control Officer or DoD Clearance Officer for this information. This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☒ Yes ☐ No ☐ Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

OMB Control Number: 0704-0415; Expiration Date: None